P2PSIP
Internet-Draft
Intended status: Informational
Expires: September 15, 2011

Y. Peng
W. Wang
ZTE Corporation
J. Peng
L. Le
China Mobile
Z. Hao
Y. Meng
ZTE Corporation

March 14, 2011

Network Management Scenarios for RELOAD
draft-peng-p2psip-network-management-scenarios-02

Abstract

The RELOAD protocol can be applied in different kinds of scenarios, including the Internet, carrier's dedicated network, enterprise network, etc. This document summarizes the network management scenarios by analyzing typical application model for each of the above three kinds of scenarios.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 15, 2011.

Copyright Notice

Table of Contents

1. Introduction

The RELOAD protocol is a peer-to-peer (P2P) signaling protocol, which provides an abstract storage and messaging service between a set of cooperating peers that form the overlay network. It can be applied in different kinds of scenarios, including the Internet, carrier's dedicated network, enterprise network, etc. This document summarizes the network management scenarios by analyzing typical application model for each of the above three kinds of scenarios.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

We use the terminology and definitions from Concepts and Terminology for Peer to Peer SIP [I-D.ietf-p2psip-concepts] and the RELOAD Base Protocol [I-D.ietf-p2psip-base] extensively in this document.

SNMP: Simple Network Management Protocol.

3. Network Management Scenarios for RELOAD Applied on The Internet

There are a variety of application models for RELOAD on the Internet, this document only analyses one of the typical application model named "Public P2P VoIP Service Providers" [cite P2PVoIP scenario]. As stated in the draft of application scenarios for RELOAD, centralized operation and management is required for RELOAD in this application model. Here we will analyse two aspects of the network management requirements for this application model.

From the viewpoint of the service provider, they need to ensure network stability and efficient operation. On the one hand, the provider needs to monitor and control their own devices, and view network utility and load of the devices; on the other hand, because of its openness to user nodes, it is necessary to prevent malicious user nodes from attacking the service network and abnormal user nodes from disturbing the service network, so the action of user nodes need be monitored and controlled. Furthermore, human intervention may be needed when the built-in mechanisms in RELOAD is not able to solve the network problems.

From the viewpoint of administrator of enterprise users who use the service from the public P2P VoIP service provider, they need to ensure their own network security, defense external network attacks

and viruses; It is needed to prevent commercial secret leakage; It is also needed to limit user function to prevent misuse enterprise VoIP services; It is needed to reasonably distribute traffic flows to improve user experience using limited bandwidth. As an example, Skype plans to provide administration tools for enterprise users to resolve the problem that Skype may be blocked by enterprise networks. (Note: This quotes from http://www.best-voip-review.com/news/2010_06_Skype_offers_network_management_tools_to_control_their_software.htmlz)

According to the above requirements, we put forward the following network management scenarios for RELOAD used on the Internet:

a. Monitoring and controlling the service provider's own devices, such as viewing and modifying the configuration parameters of the devices, monitoring the load and running state of accessed nodes(or super nodes) and the number of client nodes that access accessed nodes(client nodes include RELOAD client and application client).

b. Viewing and collecting various network data, such as routing table, the data stored in nodes, real-time status information of nodes, in order to find out the operational status of the network, such as capacity of network, quality of service, network topology information. These are the decision-making basis for optimization and adjustment of the network.

c. Alarm for abnormal events, such as congestion, message process failures, routing failures, link failures, etc.

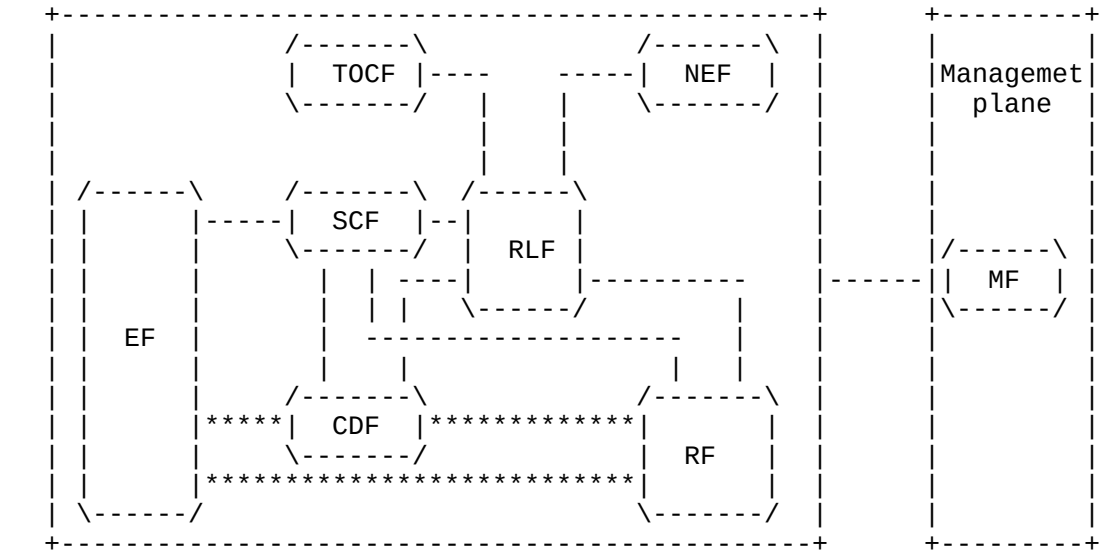
d. Disposal of abnormal nodes, for example, finding illegal user nodes and forcing it to exit the network, finding fault nodes that can't perform RELOAD related responsibilities and requiring them to rejoin or forcing them to quit. These ensure the health of the network.

e. Providing network management tool for enterprise users. The administrator of the enterprise may control specific data flow through RELOAD nodes, and limit application functions, and configure the communication port by this tool.

4. Network Management Scenarios for RELOAD Applied on Carrier's Dedicated Network

DHT-based VoIP service is studied in DSN project of ITU-T (SG13 Q19). Its architecture and processes were developed by referring RELOAD. Although it has not yet been clearly adopted which protocol will be

adopted in the project, but it is feasible that RELOAD is used here. And it is very possible that RELOAD is adopted by the VoIP service of DSN. The following figure is the architecture figure defined in DSN.



RLF in the above figure is equivalent to the peer of RELOAD. And NEF is equivalent to the Enrollment server of RELOAD. And MF is the function of network management. The specific descriptions of every function are as follows:

RLF (Resource Location Functions):

Resource registration;

Locate resources (content, Relay Node, subscription data, service capability, etc.);

Store and maintain resource information;

Routing of DSN message;

Construction and management (such as updating routing tables, transferring resources when a new node joins the overlay network, and so on.)of overlay network;

Retrieve optimization information from TOCF(Traffic Optimization Control Functions).

NEF (Node Enrolment Functions):

Provide bootstrap information for the DSN Node to join the DSN;

Assign globally unique Node ID to the DSN Nodes;

Configure parameters and information related to joining of the DSN Node;

Apply Authentication/Authorization to DSN Node;

Maintain the Node profile of all enrolled nodes (e.g. Node ID, Zone information and etc), which can be requested by RLF;

MF (Management Functions):

DSN network and service administration

DSN monitoring and diagnosis

Statistics and Accounting which includes collection of information related to usage and contribution of DSN services.

It is a telecom class application network built by telecom operators, and the Management Function is clearly defined in the architecture draft so as to achieve network management. In this kind of applications, the core network devices are provided by telecom operators. As the number of the devices is large and network topology changes frequently, it is very difficult to manage devices one by one, so the need for centralized operation and management is obvious. Moreover, the existing telecom networks were equipped with the appropriate network management systems. In this kind of application model, we will analyze the needs for network management mainly from the perspective of network operators:

Firstly, in order to ensure network stability and efficient operation, the network operators need to monitor and control the network devices to ensure utility and load of the core devices.

Secondly, the network operators need to effectively locate failure when an exception occurs in the system.

For these requirements, we propose the following specific network management scenarios:

a. Monitoring and controlling network devices. Such as viewing and modifying the configuration parameters of the devices, monitoring load and running state of the devices, controlling the functions

and roles of these devices in the network.

b. Viewing and collecting various network data, such as routing table, the data stored in nodes, real-time status information of nodes, in order to find out the operational status of the network, such as the capacity of network, the quality of service, network topology information. These are the decision-making basis for network optimization and adjustment.

c. Abnormal nodes alarm, such as congestion, message process failures, routing failures, link failures, etc.

d. When an exception occurs, the operators may find the location and the cause of failure by tracing process flow and signaling or doing diagnostic test. It will provide effective help to resolve the failure.

5. Network Management Scenarios for RELOAD Applied on Enterprise Network

RELOAD can be applied in a variety of application models in controlled private network, which was put forward in the draft of application scenarios for RELOAD. The need for centralized operation and management was clearly stated in the application model named "P2P for Redundant SIP Proxies" in this draft. This document analyses the need of network management only for this kind of application model.

Firstly, in order to ensure network stability and efficient operation, the IT department of enterprise needs to monitor and control network devices to ensure reasonable utilization rate and no overload.

Secondly, the IT department of enterprise needs to ensure the network security, to defense external network attacks and viruses; It is needed to prevent commercial secret leakage; It is needed to limit user functions to prevent misuse of network resources; It is needed to reasonably distribute traffic flows to improve the user’s experience under the limited bandwidth.

Thirdly, the network operators need to effectively locate failure when an exception occurs in the system.

For these requirements, we propose the following specific network management scenarios:

a. Monitoring and controlling the network devices, such as viewing and modifying the configuration parameters of the devices, monitoring load and running state of the accessed nodes(or super nodes) and the number of client nodes that access accessed nodes(client nodes include RELOAD Client and Application Client).

b. Viewing and collecting various network data, such as routing table, the data stored in nodes, real-time status information of nodes, in order to find out the operational status of the network, such as the capacity of the network, the quality of service, network topology information. These are the decision-making basis for optimization and adjustment of the network.

c. Abnormal nodes alarm, such as congestion, message process failures, routing failures, link failures, etc.

d. Disposal of abnormal nodes, for example, finding illegal user nodes and forcing it to exit the network, finding fault nodes that can’t perform RELOAD related responsibilities and requiring them to rejoin or forcing them to quit, and doing corresponding treatment. These ensure the health of the network.

e. The manager may control specific data flow through RELOAD nodes, and limit application functions, and configure the communication port, in order to control the actions of users.

f. When an exception occurs, the operators may find the location and the cause of failure by tracing process flow and signaling or doing diagnostic test. It will provide effective help to resolve the failure.

6. Summary of the Network Management Scenarios for RELOAD

Differences Among These Scenarios

Applications Category / Network Management Scenarios	Internet	Carrier's Dedicated Network	Enterprise Network
Applications Scenarios	"Public P2P VoIP Service Providers" in the RELOAD scenarios draft	Carrier's dedicated network application in the DSN project of ITU-T	"P2P for Redundant SIP Proxies" in the RELOAD scenarios draft
Monitoring Dedicated Device	Y	Y	Y
Viewing Network Data	Y	Y	Y
Fault Alarming	Y	Y	Y
Disposing Malicous/Fault User Nodes	Y		Y
Controlling User Node	Y		Y
Troubleshooting Quickly	Y (It is said that Skype will provide this tool to solve the problem of blocking by enterprise)	Y	Y
Control Level of Network Management	Loose	Strict	Medium

According to above analysis, we think whether RELOAD is applied on the Internet or carrier's dedicated network or enterprise network, network management is always involved in some application models and scenarios. So it is necessary to study the network management solution for RELOAD and to define its corresponding implementation protocol.

7. Relationship between Network Management Protocol and Diagnostic Protocol

A diagnostic mechanism was proposed in [I-D.ietf-p2psip-diagnostics], which is an extension to RELOAD protocol and defines the method how to monitor the connection between peers and the node status. While the SNMP usage for reload protocol focus on how to apply SNMP to manage DHT overlay considering its particular network circumstance. There are some correlations between the network management protocol and the diagnostic protocol. But they are applied respectively between different network elements. The network management protocol is used between the network management server and the managed peers. The diagnostic protocol is used between two peers in the overlay. These two protocols can fulfill network management functions through collaboration. For example, the network management server sends SNMP message to Peer to trigger diagnostic operation. After RELOAD Peer receives the message, it will do diagnostic test through RELOAD diagnostic message and generate result data. Finally, this REOAD Peer will report the diagnostic result to the network management server through SNMP message.

8. Security Considerations

The security requirements of the various application scenarios vary tremendously. They should be discussed in more detail in this document.

9. IANA Considerations

This document has no IANA Considerations.

10. Acknowledgments

This draft is based on "REsource LOcation And Discovery (RELOAD) Base Protocol" draft by C. Jennings, B. Lowekamp, E. Rescorla, S. Baset and H. Schulzrinne.

This draft make a reference to "Application Scenarios for Peer-to-Peer Session Initiation Protocol" draft by D. Bryan, E. Shim, B. Lowekamp, S. Dawkins, Ed.

Thanks to the many people of the IETF P2PSIP WG whose many drafts we have learned.

11. References

11.1. Normative References

[I-D.ietf-p2psip-app-scenarios]
Bryan, D., Shim, E., Rescorla, E., Lowekamp, B., Dawkins, S., and Ed. , "Application Scenarios for Peer-to-Peer Session Initiation Protocol", November 2007.

[I-D.ietf-p2psip-base]
Jennings, C., Lowekamp, B., Rescorla, E., Baset, S., and H. Schulzrinne, "REsource LOcation And Discovery (RELOAD)Base Protocol", November 2010.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

11.2. Informative References

[I-D.ietf-p2psip-concepts]
Bryan, D., Matthews, P., Shim, E., Willis, D., and S. Dawkins, "Concepts and Terminology for Peer to Peer SIP", July 2008.

[I-D.narten-iana-considerations-rfc2434bis]
Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", draft-narten-iana-considerations-rfc2434bis-09 (work in progress), March 2008.

[RFC2629] Rose, M., "Writing I-Ds and RFCs using XML", RFC 2629, June 1999.

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, July 2003.

Appendix A. Additional Stuff

Authors' Addresses

YongLin Peng
ZTE Corporation
Nanjing, 210012
China

Phone: +86 13776637274
Email: peng.yonglin@zte.com.cn

Wei Wang
ZTE Corporation
Nanjing, 210012
China

Phone: +86 13851658076
Email: wang.wei108@zte.com.cn

Jin Peng
China Mobile Communication Corporation
Beijing,
China

Phone: +86 13911281193
Email: pengjin@chinamobile.com

LiFeng Le
China Mobile Communication Corporation
Beijing,
China

Phone: +86 13910019925
Email: lelifeng@chinamobile.com

ZhenWu Hao
ZTE Corporation
Nanjing, 210012
China

Phone: +86 13382087596
Email: hao.zhenwu@zte.com.cn

Meng Yu
ZTE Corporation
Nanjing, 210012
China

Phone: +86 18651806839
Email: meng.yu@zte.com.cn